

Reconstruct Face from Features Using GAN Generator as a Distribution Constraint[★]

Xingbo Dong^a, Zhihui Miao^b, Lan Ma^c, Jiajun Shen^c, Zhe Jin^d, Zhenhua Guo^e, Andrew Beng Jin Teoh^{a,*}

^a*Yonsei University, Seoul, Republic of Korea*

^b*Fuzhou University, Fuzhou, China*

^c*TCL AI Lab, Shenzhen, China*

^d*Anhui University, Hefei, China*

^e*Tsinghua Shenzhen International Graduate School, Shenzhen, China*

Abstract

Face recognition based on the deep convolutional neural networks (CNN) shows superior accuracy performance attributed to the high discriminative features extracted. Yet, the security and privacy of the extracted features from deep learning models (deep features) have been often overlooked. This paper proposes the reconstruction of face images from deep features without accessing the CNN network configurations as a constrained optimization problem. Such optimization minimizes the distance between the features extracted from the original face image and the reconstructed face image. Instead of directly solving the optimization problem in the image space, we innovatively reformulate the problem by looking for a latent vector of a GAN generator, then use it to generate the face image. The GAN generator serves as a dual role in this novel framework, i.e., face distribution constraint of the optimization goal and a face generator. On top of the novel optimization task, we also propose an attack pipeline to impersonate the target user based on the generated face image. Our results show that the generated face images can achieve a state-of-the-art successful attack rate of 98.0% on LFW under type-I attack @ FAR of 0.1%. Our work sheds light on the biometric deployment to meet the privacy-preserving and security policies.

Keywords: Face recognition, template security, deep networks, deep templates, distribution constraint, GAN

1. Introduction

With the advancement of deep learning, the face has become one of the most popular biometric traits because of its convenience and superior recognition performance. However, while the deployment of face recognition (FR) facilitates the comfort and efficiency of identity management, it also evokes inevitable challenges to privacy and security because of the permanent

[★]This work was supported the Brain Pool Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT under Grant 2021H1D3A2A01099396.

*Corresponding author: Andrew Beng Jin Teoh (e-mail: bjteoh@yonsei.ac.kr).



Figure 1: We propose a novel pipeline to reconstruct high visual quality face images from their corresponding deep features by using the GAN generator as a distribution constraint and considering the feature extractor as a black box. This figure demonstrates the reconstructed face image on the colorFERET dataset (type-I); Yellow numbers are the normalized similarity scores between features of reconstructed and bona fide faces, and they are above the system’s decision threshold (0.6324) at FAR=0. Red numbers are COTS confidences (%) of being the same person compared with bona fide.

linkage of the face data and the corresponding owner’s identity. One main concern of the face recognition system is that the disclosure of face image may expose the private and sensitive information of the user, and such information can be exploited to gain illegal access to the user’s system [1, 2]. Face database breaches are not uncommon and they have been reported in the news media. For example, in 2019, 2.56 million people’s personal information, including ID cards and photos, were leaked from an AI company¹. In 2020, Clearview AI, a company that owns over 3 billion photos in the database, suffered a data breach².

On the other hand, generative adversarial networks (GANs) have actively been utilized to manipulate face images or videos for malicious purposes such as face morphing attacks, face swapping (Deepfake) etc. [3, 4, 5, 6]. Such attacks require the knowledge of the target user’s face image. On the contrary, fewer investigations have been done to reconstruct face images from the face features extracted by the deep model *without* knowing the target user’s face image.

Only a few works have previously engaged in the face images reconstruction from the face deep features³. Previous works have typically been based on convolutional networks [7] or deconvolutional neural networks [8]. Among them, [8] is specifically proposed to reconstruct the face image from its deep feature. The generated face images by [8] achieve a state-of-the-art attack success rate. However, the generated face images in [7, 8] are in low-resolution, often leaving the synthetical artifacts that can let human or machines spot easily (see Figure 5); furthermore, a GAN model is also required in [8] to generate a tremendous amount of images for the network training. In [9], a neural network is established to learn a mapping between the latent vector space of the StyleGAN2 [10] and the feature vector space of the face feature extractor. Given a feature vector, the proposed model can predict the corresponding latent vector, and high-quality face images (1024×1024) can be generated subsequently. However, the mapping method in [9] leads to the artifacts in the reconstructed face and can only achieve an attack success rate of 10.1%@1%FAR (false accept rate) when compared with bona fide (genuine) face images on the LFW dataset.

¹<https://www.biometricupdate.com/201902/facial-recognition-company-sensenets-silent-following-data-leak>

²<https://www.forbes.com/sites/kateoflahertyuk/2020/02/26/clearview-ai-the-company-whose-database-has-amassed-3-billion-photos-hacked>

³We denote features extracted from deep learning models as deep features or deep templates. They are used interchangeably.

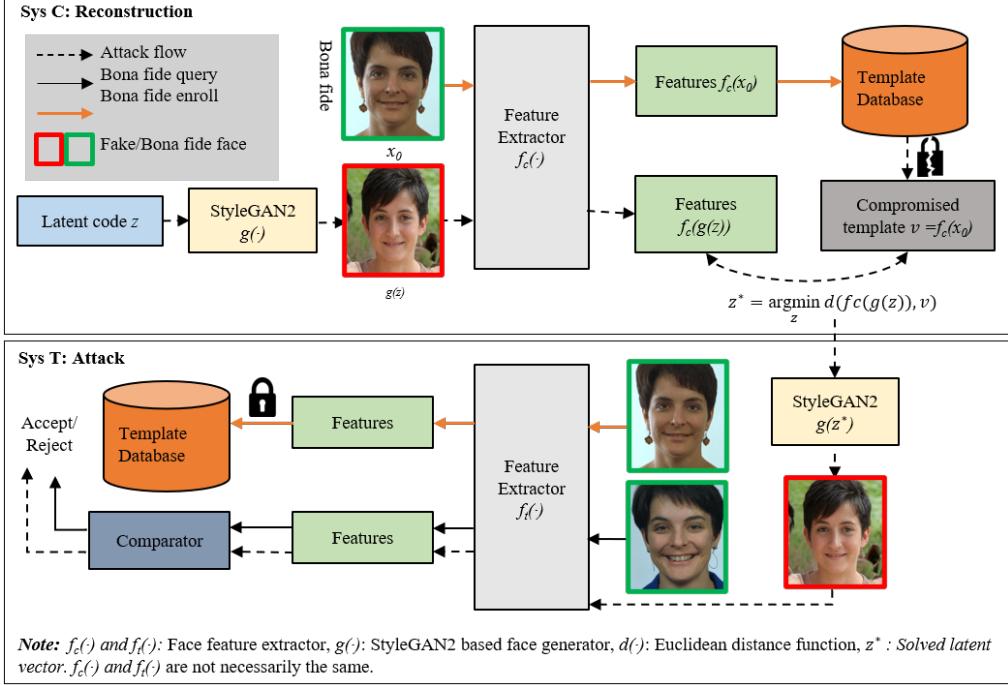


Figure 2: Overview of the framework for reconstructing face images from the corresponding compromised deep templates. The constrained optimization problem aims at solving for a latent vector in the GAN generator’s latent space, and then the latent vector is used to generate the face image. To simulate the impersonate attack, the reconstructed face images from Sys C are used to attack Sys T. The proportion of attack attempts that are falsely accepted by Sys T is evaluated as the attack performance. Sys C does not necessarily share the same feature extractor with Sys T. Best viewed in color.

Our work focuses on reconstructing face images based on deep features. We demonstrate the effectiveness of our approach by launching impersonate attacks on the face recognition system using the generated face images. More specifically, given x is the enrolled face image, and $f(\cdot)$ is the face feature extractor, we assume that the stored template $v = f(x) \in \mathcal{V}$ is known to the adversary, where \mathcal{V} denotes the feature space and x is unknown to the adversary. We also assume the deep feature extractor is a black box wherein the details of the extractor are not known to the adversary. Still, the adversary can generate unlimited input-output data pairs from the deep feature extractor. To achieve the goal mentioned above, we reformulate the face image reconstruction problem as a constrained optimization problem and explore a solution based on the Genetic Algorithm (GA). As shown in Figure 1, our method can generate high-quality images from the deep features with semantic details. Furthermore, the generated face can be utilized to access a target FR system based on the impersonate attack. The overview of the proposed pipeline is shown in Figure 2.

In summary, this paper makes the following contributions:

1. We propose a novel framework for reconstructing face images from deep features extracted by deep learning models. We first reformulate the face image reconstruction problem as a constrained optimization problem. Then, a pipeline of face image reconstruction

is proposed by searching for a latent vector in the GAN generator’s latent space, which is used to generate the face image. The GAN generator serves as a face distribution constraint of the optimization goal and a face generator. Subsequently, we adopt a Genetic Algorithm (GA) to solve the optimization problem and validate the feasibility.

2. We evaluate our reconstructed face by launching an impersonate attack to access a target face recognition system with the same or different feature extractor. Our method can achieve state-of-the-art attack performance on the LFW datasets (98.0%@0.1%FAR) and comparable performance on colorFERET datasets (76.0%@0.1%FAR).
3. The generated face images are also evaluated with three Commercial-Off-The-Shelf (COTS) face liveness detectors. The result shows that the generated high resolution face images can fool the COTS detectors with a pass rate of 88.6%, 62%, and 98%.

2. Related Work

With the rapid developments in computing hardware, big data, and novel algorithms, deep learning-based FR techniques have fostered numerous startups with practical applications in the past five years. Massive deployment of FR systems based on the deep learning models [11, 12, 13, 14, 15, 16, 17, 18] draws the public’s attention to the privacy and security concerns of reconstructing face images from deep features [19, 20]. According to the techniques used, face image reconstruction can be divided into conventional and deep learning methods. Several conventional face image reconstructions are based on the optimization algorithms, such as hill-climbing [21, 22] and radial basis function (RBF) regression [23]. On the other hand, given the adversary’s knowledge of the extractor, face image reconstruction can be classified into two main branches, i.e., white-box-based (wherein feature extractor is known) and black-box-based (wherein feature extractor is unknown) approaches. This section mainly discusses the deep learning-based methods as we focus on deep templates.

A method to invert FaceNet face embedding [11] to face images is presented in [24]. The inverting task is formulated as a minimization problem that minimizes the template difference between original and reconstructed images. To achieve this task, a regularization function based on the intermediate layer of the feature extractor is utilized. However, the detailed parameter of the extractor may not be available in reality. Later, a method to generate normalized face images is proposed [7]. Although the motivation [7] is different from reconstructing a face from features, the normalized face images are generated from the FaceNet features based on differentiable image warping by combining landmark and texture information. However, the landmark and texture information is required, and the last convolution layer of the extractor is also utilized in the pipeline, which may be impractical in reality for face image reconstruction.

A de-convolutional neural network is used in [8] to achieve the face image reconstruction task because of its up-sampling capability. In [8], the feature extractor is regarded as a black box that the adversary does not necessarily know. A cascade of multiple stacked de-convolution blocks and a convolution block, namely neighborly de-convolutional neural network (NbNet), is designed to generate the output face images. GAN synthesizes face images, and two benchmark face datasets are utilized for training the NbNet. The experiment results indicate that 95.20% of the generated face images can successfully access the face recognition system enrolled with the same face image at an FAR of 0.1% (type-I attack in [8]). Later in [25], by utilizing the NbNet, the authors propose to reconstruct the face image from a binary template produced by a given binarization method. Other methods, such as iterative sampling of random Gaussian blobs [26]

and autoencoder [27], have also been reported in the literature. However, those methods can only produce low-resolution and vision-unfriendly images which the naked eye can easily spot.

In [9], a framework to reconstruct high-quality face images from deep features is proposed. A neural network is established to learn a mapping between the latent vector space of the StyleGAN2 [10] and the feature vector space of the face feature extraction model. Given a feature vector, the model predicts the corresponding latent vector, and face images can be generated subsequently. However, the work based on the vanilla fully connected neural network [9] is suboptimal for this task. The stochastic gradient descent algorithm can be trapped in a local minimum. Hence, the method can only achieve a successful attack rate of 10% on LFW under type-I attack @1%FAR. As a result, most reconstructed face images show poor visual similarity compared with the Bona fide face images (see Figure 4).

One shortcoming of the methods mentioned above is that only low-resolution face images can be generated. For instance, the output image size in [8] is 160×160, and the size in [7, 24] is 224×224. 224 may be enough for face recognition and liveness detection, but higher resolution is usually preferred and considered a prerequisite for face recognition [28, 29, 30]. On the other hand, although face image reconstruction has been achieved in [9], tremendous artifacts exist, and the attack success rate still leaves a large room for improvement (see **section 4.2**). To address the discussed problems, we reformulate the face reconstruction task as a novel constrained optimization problem and solve it by GA due to its population-based evolution property; hence, highly visually similar face images reconstructed from their corresponding features can be achieved.

3. Face Reconstruction on Generator-based Distribution Constraint

In this work, we assume that the stored template $v = f(x_0) \in \mathcal{V}$ is known to the adversary, where \mathcal{V} denotes the feature space and x_0 is the registered face images. We highlight that big quantities of templates can be compromised and available to the adversarial systems, but we focus on **single compromised template** case. We also assume that the adversary can exploit the deep feature extractor $f(\cdot)$ to generate unlimited input-output data pairs. However, the deep feature extractor is regarded as a black box that is not necessarily known to the adversary. Finally, it is worth pointing out that *we assume that images of the target person are not used to train the target face recognition system*.

The goal of the adversary is to reconstruct a **visually similar** face image x^* from the compromised template v ; meanwhile the features extracted from x^* should be **closer** to the original feature v . The goal is formulated as:

$$\begin{aligned} x^* &= \arg \min_x d(f(x), v), \\ s.t. \quad x &\in X, \end{aligned} \tag{1}$$

where $d(\cdot)$ is a distance function (e.g., Euclidean distance), $f(\cdot)$ indicates a deep learning-based feature extraction function and $v = f(x_0)$ is the compromised template in the database, and X denotes the domain of human face. Note that other feature extractors such as LBP [31, 32] and HOG [33], can also be used, as we treat it as a black box.

One challenge for the above optimization goal is how to impose a constraint to the x , i.e., constraining the x_0 to be a human face. One naive way is representing the constraint in terms of

Algorithm 1: Solving the latent vector by GA.

INPUT: Compromised template v

Face generator g

Face encoder f

GA population size t

GA selection rate s

OUTPUT: Solved latent vector z^*

Randomly initiate GA population as $Z = \{z_i | i = 1, 2, \dots, t\}$

repeat

Step1: Generate face images $X = \{g(z_i) | i = 1, 2, \dots, t\}$;

Step2: Generate deep features $V = \{f(g(z_i)) | i = 1, 2, \dots, t\}$;

Step3: Compute the distance $d(f(g(z)), v)$ as the fitness value for each z ;

Step4: Top $s \times t$ best z are selected as the parents $Z_{parents}$ of next generation;

Step5: Generate new child $Z_{children}$ by crossover and mutation operations on the $Z_{parents}$;

Step6: Generate the next generation population: $Z = \{Z_{parents}, Z_{children}\}$;

until converged;

Step7: return the best individual of the last generation population as z^* .

probability distribution:

$$\begin{aligned} \mathbf{x}^* &= \arg \min_{\mathbf{x}} d(f(\mathbf{x}), v), \\ s.t. \quad \mathbf{x} &\sim P_{face}(x), \end{aligned} \tag{2}$$

where $P_{face}(x)$ denotes the distribution of face images. However, as $P_{face}(x)$ cannot be explicitly defined, it remains challenging to incorporate $P_{face}(x)$ directly into the optimization objective function when solving the above problem. Motivated by GAN's distribution modeling capability[34, 35, 36, 37, 38], we propose to relax the above optimization function by transferring the optimization solution space from the image space to the GAN's latent space. Generative models, such as StyleGAN [39, 10], learn a mapping relationship between the prior distribution $\pi(z)$ and the training set's pixel probability distribution $p(x)$. The prior distribution $\pi(z)$ is usually a Gaussian distribution, and the generator's output follows the distribution of face images. Since StyleGAN is powerful for face generation, we opt for StyleGAN2 [10] generator as the constraint of the optimization goal. Hence Eq.(2) can be reformulated as:

$$\begin{aligned} \mathbf{z}^* &= \arg \min_z d(f(g(z; \theta)), v), \\ s.t. \quad z &\sim \mathcal{N}(0, I), \\ P_{g(z; \theta)} &\approx P_{face}(x), \end{aligned} \tag{3}$$

where θ is the parameter of StyleGAN2, $g(\cdot)$ indicates a pre-trained StyleGAN2 based face generation model function. The constraint $\mathbf{x} \sim P_{face}(x)$ in Eq. (2) is eliminated at the cost of a strong assumption $P_{g(z; \theta)} \approx P_{face}(x)$; in another word, we assume that the distribution of well-trained generator's output image $P_{g(z; \theta)}$ resembles real human face distribution $P_{face}(x)$, i.e.,

$P_{g(z;\theta)} \approx P_{face}(x)$. The optimization goal is now looking for the best latent vector z , which is more easily operated.

As opposed to [8] and [9], we aim at reconstructing high visual quality and similarity with the bona fide face images. We propose a novel way to achieve template inverting tasks of Eq. (3) by incorporating a standard Genetic Algorithm (GA)[40]. The detailed processing pipeline is shown in Algorithm 1.

As the investigation [41] suggests, the latent code of well-trained generative models learns a disentangled representation. Given the GA’s ability to search for the best solution with a vast population of candidates representing the various face attribute combinations pulled from the latent vector, GA is preferable for the above-formulated problem.

4. Experiments and Results

4.1. Settings

In our experiment, a pre-trained StyleGAN2 model⁴ is adopted. The pre-trained model is trained on the FFHQ dataset [39], consisting of 70,000 high-quality images at 1024×1024 resolution. We trained three InsightFace models with different backbones, including ResNet-50, Xception, and InceptionResNet on MS-celeb-1m dataset [42] in our experiments.

To evaluate the performance of the proposed method, the Labeled Faces in the Wild (LFW) [43, 44], and color FERET (colorFERET) [45, 46] datasets are adopted in our experiments. LFW and colorFERET are selected as they represent unconstrained or semi-constrained environments: 1) face images in LFW are collected from the Internet and are usually captured in unconstrained environments; 2) face images in the color FERET database are captured in a semi-controlled environment with 13 different poses.

To initiate the GA, the default population size was set to 256 individuals, and the selection rate was set at 0.3; while the mutation ratio was set at 0.3, the cross-over point is selected randomly. The mutation is performed by adding a random number drawn from a standard Gaussian distribution to each entry of the parent vector. The algorithm ends if the fitness value does not decrease for the last 20 generations or the algorithm has already reached 1000 generations.

To simulate the attack risks, in reality, two simulation scenarios [47] are adopted as below (also see Figure 2):

Compromised system (*Sys C*): This is a biometric system compromised by the adversary. In this subsystem, we assume that 1) the stored template $v = f_c(\mathbf{x}_0)$ of the target user is compromised by the adversary; 2) the deep feature extractor can be utilized by the adversary to generate unlimited input-output data pairs; 3) the deep feature extractor is a black-box to the adversary in that the adversary does not necessarily know the parameters. InsightFace model with ResNet-50 backbone is adopted as the feature extractor in *Sys C*.

Targeted system (*Sys T*): This is a biometric system subject to a reconstruction attack. Each user’s reconstructed face image $\hat{\mathbf{x}}$ from a template stored in the *Sys C* was generated and used to break into *Sys T* as shown in Figure 2. The feature extractor $f_f(\cdot)$ used in the *Sys T* could be different from *Sys C*, and the user’s enrolled image could also be different from *Sys C*. We consider both cases in our subsequent experiment. Three InsightFace models with ResNet-50, InceptionResNet, and Xception backbone are adopted as the candidate feature extractors in *Sys T*.

⁴<https://nvlabs-fi-cdn.nvidia.com/StyleGAN2/networks/StyleGAN2-ffhq-config-f.pkl>

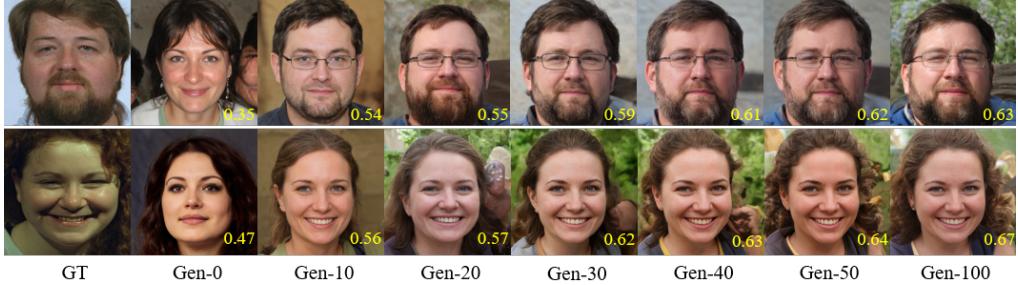


Figure 3: Visual demonstration of the evolution of the GA. GT refers to the ground truth face images, and images with normalized similarity score (yellow number) are the best candidate images (type-I) selected at the i -th generation (Gen- i) of the GA.

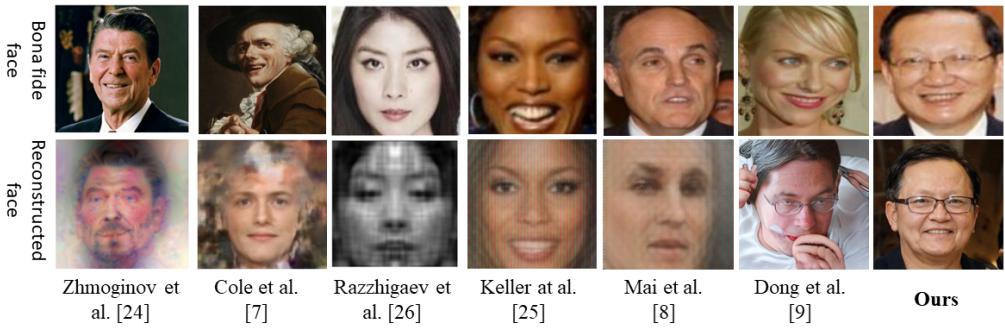


Figure 4: Comparison of visual quality with existing works.

Each user’s face image is reconstructed in the attack simulation based on one compromised template in $Sys\ C$. Then, three GA threads are initiated for each user simultaneously, and the best individual candidate among the three threads is selected to reconstruct the final face image. Subsequently, in $Sys\ T$, the face template is extracted from the reconstructed face image. Finally, three types of similarity scores are calculated: 1) **mated-attack score** is computed by comparing reconstructed face features with the real **mated** face of the same person; 2) **genuine scores** are computed as the similarity between bona fide features from the same person; and 3) **impostor scores** are computed as the similarity between bona fide features from different persons.

The successful attack rate (SAR) is calculated as the proportion of mated-attack attempts that are falsely declared to match the template of the same user at the given similarity threshold under different FAR, i.e., the ratio of mated-attack scores above the similarity threshold. The threshold is determined based on the normal genuine and imposter scores. SAR can be regarded as the false match rate under attack, and a higher SAR implies the higher performance of the reconstruction attack and vice versa. Similar to [8], when the real template is from the same compromised face image in $Sys\ C$, the attack is referred to as a type-I attack. When the real template is from the different face images of the same person, the attack is regarded as a type-II attack.

4.2. Qualitative Evaluation

We first examine the effectiveness of the genetic algorithm. Examples of the generated face images from the 0th to 100th generation of GA are shown in Figure 3. We can find that although

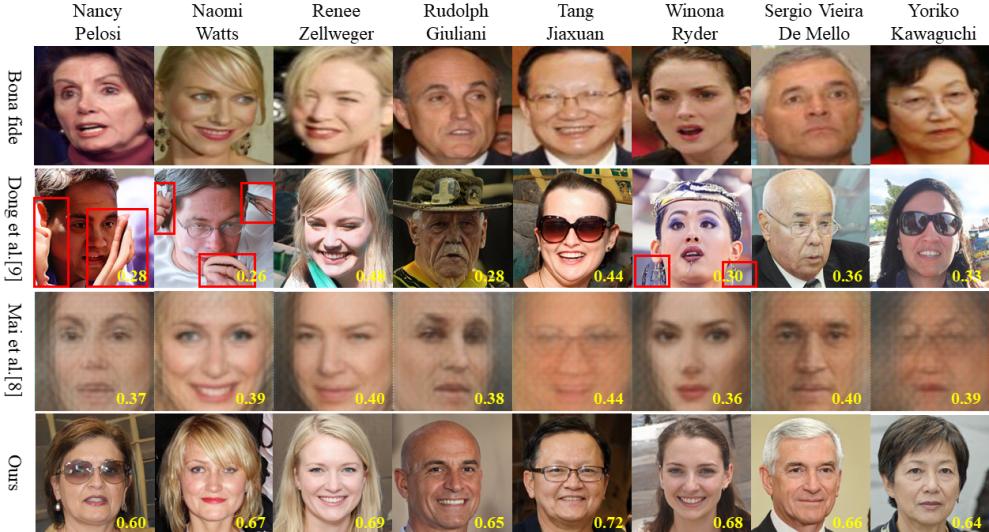


Figure 5: Visual demonstration of reconstructed face images from the LFW dataset (type-I). **Yellow** numbers are the normalized similarity scores between features of the corresponding image and bona fide face, they are above the FAR=0 decision threshold (0.5212), and red boxes indicate the artifacts caused by sub-optimal latent codes produced by [9].

images in the initial generation show distinct faces, as the GA manages to search for an optimal latent vector, the algorithm can generate faces visually similar to the corresponding bona fide images as the generation evolves. As Figure 3 suggests, 20 generations of evolution are enough to produce visually similar fake face images. Furthermore, the similarity between the target and face templates increases as the generation evolves. For example, as Figure 3 shows, the fitness value can increase to 0.63 from 0.35 for the first user in the first row. This indicates that the proposed framework is effective and efficient.

Next, a comparison of image visual quality with existing works is shown in Figure 4. Compared with [24, 7, 26, 25, 8], our generated face images have higher visual quality and higher resolution. Though high resolution images can be generated by [9], but many artifacts are founded.

Examples of bona-fide images and their generated face images based on randomly selected subjects in colorFERET and LFW are shown in Figure 1 and Figure 5. The final succeeded fake face instances show high visual similarity compared with the corresponding bona fide images on both LFW and colorFERET datasets. The visual results indicate that the proposed method can generate high-quality and similar face images from the corresponding face features with StyleGAN’s generator. Additionally, compared with [8], our generated face images have higher visual quality and higher resolution. However, many artifacts are founded on [9] because of sub-optimal latent codes produced by [9]; additionally, better visual similarity can be observed in the images generated by our proposed novel pipeline.

We further evaluate the generated images from colorFERET with one COTS⁵ face comparator, and the confidence that the images belong to the same person is also shown in Figure 1. The results suggest that our reconstructed high quality face images can fool even COTS.

⁵<https://www.faceplusplus.com.cn/face-comparing/>

4.3. Quantitative Evaluation

We also quantitatively evaluate the performance of the proposed reconstruction scheme based on type-I and type-II attacks with the same and different feature extractors. We first compute the true accept rate (TAR) at FAR on the deep features under the normal situation in *Sys T*. Specifically, in the LFW dataset, 50 users with at least 10 images are selected randomly to compute the FAR and TAR, while in colorFERET, 50 users with at least two images are selected randomly. Then, in the reconstruction process, 50 users from LFW and 50 from colorFERET are chosen randomly to perform the face image reconstruction attack. The SARs of type I and II attacks are evaluated subsequently, and the results are shown in Table 1.

Table 1: Attack performance in Sys T with a insightFace model on various backbones (Threshold is normalized between 0 to 1).

Dataset	FAR(%)	Standard TAR(%)	Threshold	Type-I SAR(%)	Type-II SAR(%)
Resnet-50 backbone (same extractor)					
LFW	0.00	26.03	0.5212	86.00	13.63
	0.10	50.28	0.4734	98.00	29.37
	1.00	73.61	0.4300	100.00	50.92
	10.00	92.66	0.3780	100.00	76.06
color FERET	0.00	58.66	0.6324	38.00	13.44
	0.10	75.63	0.5874	76.00	39.25
	1.00	90.79	0.5310	88.00	64.52
	10.00	99.10	0.4540	100.00	91.94
Xception backbone (different extractor)					
LFW	0.00	91.90	0.4933	22.00	12.15
	0.10	97.76	0.4463	40.00	26.43
	1.00	99.41	0.4018	58.00	42.27
	10.00	99.90	0.3522	76.00	61.88
color FERET	0.00	99.64	0.5078	6.00	6.99
	0.10	99.82	0.4819	8.00	9.14
	1.00	100.00	0.4300	34.00	32.26
	10.00	100.00	0.3738	66.00	61.29
InceptionResNet backbone (different extractor)					
LFW	0.00	79.77	0.5316	4.00	2.12
	0.10	98.12	0.4382	38.00	25.32
	1.00	99.42	0.3999	52.00	38.21
	10.00	99.86	0.3522	68.00	59.39
color FERET	0.00	99.46	0.528	4.00	2.69
	0.10	100.00	0.4655	22.00	13.44
	1.00	100.00	0.4239	46.00	39.78
	10.00	100.00	0.3712	76.00	67.74

We first examine the attack performance in Sys T with the same feature extractor as Sys C, i.e., InsightFace with ResNet-50 backbone. As shown in Table 1, both type-I and type-II attacks can achieve remarkable SARs under this setting. Even at 0% FAR, the SAR can reach 86% and

13.63% for type-I and type-II attacks on LFW, respectively. The result from Table 1 suggest the proposed reconstruction scheme is effective in Sys T when using the same feature extractor as Sys C.

Next, we evaluate the attack performance in Sys T with different feature extractors, including the Xception backbone-based InsightFace model and InceptionResNet backbone-based InsightFace model. As the results of the Xception and InceptionResNet backbones from Table 1 suggest, the proposed scheme can achieve good attack performance in both cases. Specifically, for the Xception-based extractor, 40% and 26.43% of the attempts can be successful under type-I and type-II attacks under 0.1% FAR, respectively. For the InceptionResNet-based extractor, 38% and 25.32% of the attempts succeed in the type-I and type-II attacks under 0.1% FAR on LFW, respectively. It is also worth noting that type-II attacks in both cases achieve comparable SARs, which validates the proposed reconstruction scheme’s effectiveness. Furthermore, the results on colorFERET show similar promising performance, as indicated in Table 1.

The normalized similarity score distributions of the genuine pairs, imposter pairs, and mated-attack pairs are shown in Figure 6. There is a gap between the distribution of the mated-attack scores generated from the reconstructed face images and the normal imposter score distribution. Specifically, when the attack is performed upon the same feature extractor, i.e., the ResNet-50, there is considerable overlap between the attack imposter score distribution and the genuine score distribution. On the other hand, an overlap exists between the attack imposter score distribution and genuine score distribution for type-II attacks under different feature extractors. The result from Figure 6 indicates the effectiveness of our proposed method in terms of the similarity score distribution. Note that face recognition models with various backbones are different from the original InsightFace paper, hence the genuine and imposter has a overlap area.

The receiver operator characteristic (ROC) curves of type-I and type-II attacks on LFW and colorFERET are shown in Figure 7. The original ROC curve under a normal situation is also included in the graph. The results show that both type-I and type-II attacks can achieve remarkable performance in Sys T when using the same feature extractor with Sys C (see Figure 7(a,d)). Meanwhile, the proposed scheme can also achieve a good attack performance when different feature extractors with Sys C are applied (see Figure 7(b,c,e,f)).

A comparison with current state-of-the-art schemes can be found in Table 2. We include the most recent closely-related state-of-the-art works, i.e., [8, 25, 9], in our comparison. [7] is not included as it is originally designed to generate frontal and neutral expression face images under white-box setting. [24, 26] are also not included due to the lack of attack performance data from the original paper. Compared with [8], face images can be produced in our pipeline without model training. Compared with [9], the attack success rate has been boosted remarkably on the LFW dataset. Though [8, 25] can achieve better performance under Type-II attack setting, the generated images suffer from poor resolution quality.

4.4. Commercial-Off-The-Shelf liveness detection evaluation

To further validate the advantage of the reconstructed face images, three COTS liveness detection cloud computing APIs from Asia and Europe areas⁶ are used to evaluate the generated face images. The selected API depends solely upon a single RGB image for input. Different

⁶<https://ai.baidu.com/tech/face/faceliveness>;
<http://facebody.cn-shanghai.aliyuncs.com/?Action=DetectLivingFace>;
<https://skybiometry.com/demo/face-detect/> (threshold 50%)

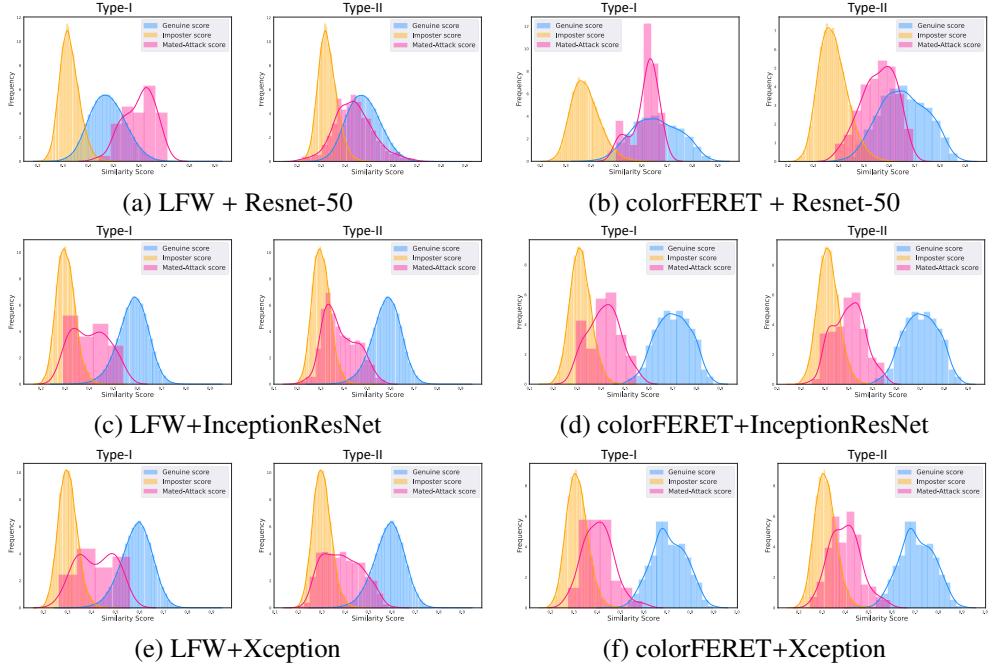


Figure 6: Distribution of the normalized similarity score of type-I and type-II attack on different datasets and different extractor backbones. (a) LFW and Resnet-50; (b) colorFERET and Resnet-50; (c) LFW and InceptionResNet; (d) colorFERET and InceptionResNet; (e) LFW and Xception; (f) colorFERET and Xception;

COTSs return different detection suggestions, but the detection results typically include the liveness scores and thresholds under various false reject rates. COTS 2 also produces suggestions for spoofing detection. COTS 3 produces liveness confidence for each image. Therefore, 150 reconstructed images from LFW are selected for evaluation. Furthermore, 150 random images were reconstructed from LFW, based on the methods [8] and [9], and are also selected for the same evaluation. The detailed results are shown in Table 3.

4.5. Ablation Study

There are three basic parameters of GA, i.e., population size, selection rate (crossover ratio), and mutation ratio. The population size determines how many individuals (the latent vectors) are in the population (in one generation). The selection rate determines how often crossover will occur, while the mutation ratio determines how often parts of an individual are mutated.

To find the best population size, we set the crossover probability to 0.2 and the mutation ratio to 0.1. The fitness value in terms of mean square error (MSE) is evaluated at different ranges (16,32,64,128,256) of population size. The lower the MSE, the better performance is achieved. As shown in Figure 8 (a), the MSE decreases while the population size increases. Generally, a smaller population size leads to smaller search space. When the population size becomes large, GA requires more computational overhead and more time is needed. We notice that the 256 population size can perform well; meanwhile, the computation time and memory requirement remain acceptable.

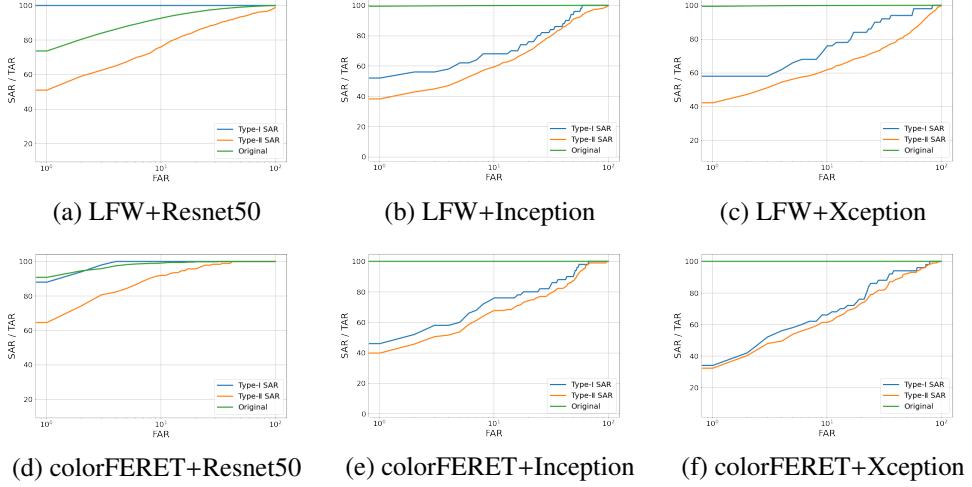


Figure 7: ROC curves of type-I and type-II attack on LFW and colorFERET with various feature extractors in Sys T (FAR is logarithmic scaled).

Table 2: Comparison with the state-of-the-art methods

Method	Property	Feature extractor	Res.	Type-I attack on LFW @ 0.1%FAR	Type-II attack on LFW @ 0.1%FAR
Mai et al. [8]	Neighborly de-convolutional neural network (NbNet) trained on GAN-generated images	Facenet	160 × 160	95.20% (VGG-NbA-P)	53.91% (VGG-NbA-P)
Keller et al. [25]	Neighborly de-convolutional neural network (NbNet)	Facenet	160 × 160	95.16% (Unprotected)	65.05% (Unprotected)
Dong et al. [9]	Mapping between latent space and feature space	InsightFace	1024 × 1024	1.42%	0.46%
Ours	GAN's distribution modeling as a constraint of the optimization task, solved by GA	InsightFace	1024 × 1024	98.00%	29.37%

Table 3: Liveness and spoofing detection by COTS.

Scheme	API	Detection Details (150 images)
Dong et al. [9]	COTS 1	pass: 77, blocked: 17, need manual review: 56
	COTS 2	pass: 41 , block: 109, not spoofing: 3, spoofing: 147
	COTS 3	pass: 138, block: 12
Mai et al. [8]	COTS 1	pass:0, blocked:93, need manual review: 57
	COTS 2	pass: 71, block: 79, not spoofing: 150, spoofing:0
	COTS 3	pass: 0, block: 150
Ours	COTS 1	pass: 133, blocked: 3, need manual review:14
	COTS 2	pass: 93, blocked: 57, is spoofing:2, not spoofing: 148
	COTS 3	pass: 147, block: 3

To determine the best crossover ratio, we set the population size to 256 and the mutation

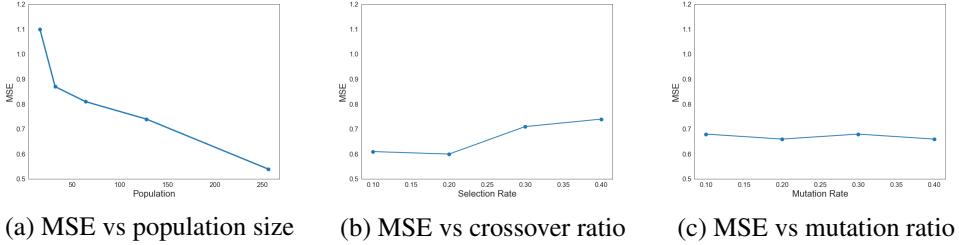


Figure 8: Ablation study on population size, crossover ratio, and mutation ratio.



Figure 9: Failure cases.

ratio to 0.1. The fitness value is evaluated under various crossover ratio values (0.1, 0.2, 0.3, 0.4). As shown in Figure 8 (b), the best performance is achieved on 0.2. Similarly, the MSE under different mutation rates is shown in Figure 8 (c); we can conclude that the impact of mutation rates with respect to the performance is not significant, so set the mutation ratio to 0.1.

4.6. Failure cases

Several typical failure cases are shown in Figure 9. In some failure cases, the fake face images are evolved easily into a baby. In other cases, the face images are evolved into female images. The failure of those cases is mainly the consequence of the generator’s modeling bias, as the dataset used to train the StyleGAN may not be well balanced.

5. Discussion and Conclusion

In this paper, a method to generate face images from deep features has been presented. The reconstruction problem is formulated as a task to find the best latent vector of a pre-trained StyleGAN model, which can be utilized to generate a face image visually similar to the target face image. The generator is used as a human face constraint to the optimization task, and we propose to solve it with a genetic algorithm. Our experiment results prove that the generated face images show high similarity with the target face. We also utilize the generated face images to simulate type-I and type-II attacks on the LFW and colorFERET datasets. The quantitative results validate that the reconstructed face images can achieve a state-of-the-art attack success rate on the LFW dataset and comparable performance on colorFERET datasets.

Three COTS liveness detection APIs are adopted to evaluate the generated face images. The results show that 88.6% (62%, 98%) of generated images can pass the liveness detector COTS

1 (COTS 2, COTS3). This implies that the current COTS single photo-based liveness detection API in the market may not be safe enough.

The forged face images in this work can shed light on current face recognition systems' security and privacy risks. The adversary could potentially exploit the generated face images to gain illegal access to the face recognition systems. Besides, using the GAN generator as an explicit distribution constraint proves to be effective and straightforward in our work; hence it can be potentially generalized to related constraint optimization tasks, e.g., inverting output to input.

It is worth pointing out that the proposed approach can also be applied to other privacy- and security-sensitive features such as text and video. To mitigate such risks, template protection schemes can be utilized to protect privacy- and security-sensitive data and better anti-spoofing detection are needed to avoid such risks.

References

- [1] V. M. Patel, N. K. Ratha, R. Chellappa, Cancelable biometrics: A review, *IEEE Signal Processing Magazine* 32 (5) (2015) 54–65.
- [2] M. Gomez-Barrero, J. Galbally, Reversing the irreversible: A survey on inverse biometrics, *Computers & Security* 90 (2020) 101700.
- [3] Deepfakes, Deepfakes/faceswap: Deepfakes software for all, github.com/deepfakes/faceswap (2017).
- [4] P. Isola, J.-Y. Zhu, T. Zhou, A. A. Efros, Image-to-image translation with conditional adversarial networks, in: *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 1125–1134.
- [5] I. Korshunova, W. Shi, J. Dambre, L. Theis, Fast face-swap using convolutional neural networks, in: *Proceedings of the IEEE international conference on computer vision*, 2017, pp. 3677–3685.
- [6] Y. Nirkin, I. Masi, A. T. Tuan, T. Hassner, G. Medioni, On face segmentation, face swapping, and face perception, in: *2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018)*, IEEE, 2018, pp. 98–105.
- [7] F. Cole, D. Belanger, D. Krishnan, A. Sarna, I. Mosseri, W. T. Freeman, Synthesizing normalized faces from facial identity features, in: *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 3703–3712.
- [8] G. Mai, K. Cao, P. C. Yuen, A. K. Jain, On the reconstruction of face images from deep face templates, *IEEE transactions on pattern analysis and machine intelligence* 41 (5) (2018) 1188–1202.
- [9] X. Dong, Z. Jin, Z. Guo, A. B. J. Teoh, Towards generating high definition face images from deep templates, in: *2021 International Conference of the Biometrics Special Interest Group (BIOSIG)*, IEEE, 2021, pp. 1–11.
- [10] T. Karras, S. Laine, M. Aittala, J. Hellsten, J. Lehtinen, T. Aila, Analyzing and improving the image quality of StyleGAN, in: *Proc. CVPR*, 2020.
- [11] F. Schroff, D. Kalenichenko, J. Philbin, Facenet: A unified embedding for face recognition and clustering, in: *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2015, pp. 815–823.
- [12] J. Deng, J. Guo, N. Xue, S. Zafeiriou, Arcface: Additive angular margin loss for deep face recognition, in: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2019, pp. 4690–4699.
- [13] O. M. Parkhi, A. Vedaldi, A. Zisserman, Deep face recognition, in: *British Machine Vision Conference*, 2015.
- [14] W. Ouyang, X. Wang, X. Zeng, S. Qiu, P. Luo, Y. Tian, H. Li, S. Yang, Z. Wang, C.-C. Loy, et al., Deepid-net: Deformable deep convolutional neural networks for object detection, in: *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2015, pp. 2403–2412.
- [15] W. Liu, Y. Wen, Z. Yu, M. Li, B. Raj, L. Song, Sphereface: Deep hypersphere embedding for face recognition, in: *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 212–220.
- [16] Y. Wen, K. Zhang, Z. Li, Y. Qiao, A discriminative feature learning approach for deep face recognition, in: *European conference on computer vision*, Springer, 2016, pp. 499–515.
- [17] X. Zhang, Z. Fang, Y. Wen, Z. Li, Y. Qiao, Range loss for deep face recognition with long-tailed training data, in: *Proceedings of the IEEE International Conference on Computer Vision*, 2017, pp. 5409–5418.
- [18] H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong, J. Zhou, Z. Li, W. Liu, Cosface: Large margin cosine loss for deep face recognition, in: *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 5265–5274.
- [19] R. Ranjan, S. Sankaranarayanan, A. Bansal, N. Bodla, J.-C. Chen, V. M. Patel, C. D. Castillo, R. Chellappa, Deep

- learning for understanding faces: Machines may be just as good, or better, than humans, *IEEE Signal Processing Magazine* 35 (1) (2018) 66–83.
- [20] M. Wang, W. Deng, Deep face recognition: A survey, *Neurocomputing* (2020).
 - [21] A. Adler, Sample images can be independently restored from face recognition templates, in: CCECE 2003—Canadian Conference on Electrical and Computer Engineering. Toward a Caring and Humane Technology (Cat. No. 03CH37436), Vol. 2, IEEE, 2003, pp. 1163–1166.
 - [22] Y. C. Feng, M.-H. Lim, P. C. Yuen, Masquerade attack on transform-based binary-template protection based on perceptron learning, *Pattern Recognition* 47 (9) (2014) 3019–3033.
 - [23] A. Mignon, F. Jurie, Reconstructing faces from their signatures using rbf regression, in: British Machine Vision Conference 2013, 2013, pp. 103–1.
 - [24] A. Zhmoginov, M. Sandler, Inverting face embeddings with convolutional neural networks, arXiv preprint arXiv:1606.04189 (2016).
 - [25] D. Keller, M. Osadchy, O. Dunkelman, Inverting binarizations of facial templates produced by deep learning (and its implications), *IEEE Transactions on Information Forensics and Security* 16 (2021) 4184–4196.
 - [26] A. Razzhigaev, K. Kireev, E. Kaziakhmedov, N. Tursynbek, A. Petushko, Black-box face recovery from identity features, in: European Conference on Computer Vision, Springer, 2020, pp. 462–475.
 - [27] S. Ahmad, B. Fuller, Resist: Reconstruction of irises from templates, in: 2020 IEEE International Joint Conference on Biometrics (IJCB), IEEE, 2020, pp. 1–10.
 - [28] Z. Lu, X. Jiang, A. Kot, Deep coupled resnet for low-resolution face recognition, *IEEE Signal Processing Letters* 25 (4) (2018) 526–530.
 - [29] P. Li, L. Prieto, D. Mery, P. J. Flynn, On low-resolution face recognition in the wild: Comparisons and new techniques, *IEEE Transactions on Information Forensics and Security* 14 (8) (2019) 2000–2012.
 - [30] A. Jourabloo, Y. Liu, X. Liu, Face de-spoofing: Anti-spoofing via noise modeling, in: Proceedings of the European conference on computer vision (ECCV), 2018, pp. 290–306.
 - [31] W. Deng, J. Hu, J. Guo, Compressive binary patterns: Designing a robust binary face descriptor with random-field eigenfilters, *IEEE transactions on pattern analysis and machine intelligence* 41 (3) (2018) 758–767.
 - [32] T. Ahonen, A. Hadid, M. Pietikainen, Face description with local binary patterns: Application to face recognition, *IEEE transactions on pattern analysis and machine intelligence* 28 (12) (2006) 2037–2041.
 - [33] N. Dalal, B. Triggs, Histograms of oriented gradients for human detection, in: 2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05), Vol. 1, Ieee, 2005, pp. 886–893.
 - [34] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio, Generative adversarial nets, *Advances in neural information processing systems* 27 (2014).
 - [35] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, A. A. Bharath, Generative adversarial networks: An overview, *IEEE Signal Processing Magazine* 35 (1) (2018) 53–65.
 - [36] C. Li, H. Liu, C. Chen, Y. Pu, L. Chen, R. Henao, L. Carin, Alice: Towards understanding adversarial learning for joint distribution matching, *Advances in Neural Information Processing Systems* 30 (2017) 5495–5503.
 - [37] X. Mao, Q. Li, H. Xie, R. Y. Lau, Z. Wang, S. Paul Smolley, Least squares generative adversarial networks, in: Proceedings of the IEEE international conference on computer vision, 2017, pp. 2794–2802.
 - [38] I. Goodfellow, Nips 2016 tutorial: Generative adversarial networks, arXiv preprint arXiv:1701.00160 (2016).
 - [39] T. Karras, S. Laine, T. Aila, A style-based generator architecture for generative adversarial networks, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019, pp. 4401–4410.
 - [40] M. Srinivas, L. M. Patnaik, Genetic algorithms: A survey, *computer* 27 (6) (1994) 17–26.
 - [41] Y. Shen, J. Gu, X. Tang, B. Zhou, Interpreting the latent space of gans for semantic face editing, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020, pp. 9243–9252.
 - [42] Y. Guo, L. Zhang, Y. Hu, X. He, J. Gao, Ms-celeb-1m: A dataset and benchmark for large-scale face recognition, in: European conference on computer vision, Springer, 2016, pp. 87–102.
 - [43] G. B. Huang, M. Mattar, T. Berg, E. Learned-Miller, Labeled faces in the wild: A database forstudying face recognition in unconstrained environments, in: Workshop on Faces in 'Real-Life' Images: Detection, alignment, and recognition, 2008.
 - [44] G. B. H. E. Learned-Miller, Labeled faces in the wild: Updates and new reporting procedures, Tech. Rep. UM-CS-2014-003, University of Massachusetts, Amherst (May 2014).
 - [45] P. J. Phillips, H. Wechsler, J. Huang, P. J. Rauss, The feret database and evaluation procedure for face-recognition algorithms, *Image and vision computing* 16 (5) (1998) 295–306.
 - [46] P. J. Phillips, H. Moon, S. A. Rizvi, P. J. Rauss, The feret evaluation methodology for face-recognition algorithms, *IEEE Transactions on pattern analysis and machine intelligence* 22 (10) (2000) 1090–1104.
 - [47] X. Dong, Z. Jin, A. B. J. Teoh, M. Tistarelli, K. Wong, On the security risk of cancelable biometrics, arXiv preprint arXiv:1910.07770 (2019).